

**Listing of Claims**

This listing of claims replaces all prior versions, and listings, of claims in the application:

1. (Currently Amended) A method for automatically identifying common content to use in identifying an intrusive network attack, comprising:

obtaining a portion collection of data items to be analyzed to determine identify [[a]] the network attack;  
carrying out a data reduction reducing said data items  
[[on]] in said portion collection to reduce said data portion collection to a reduced data portion in a repeatable manner  
collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a  
constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item; and

analyzing a plurality of said reduced data portions items to detect common elements within said reduced data portion, said analyzing reviewing for common content indicative of a network attack.

2. (Currently Amended) A method as in claim 1, wherein said analyzing ~~common content~~ comprises determining frequently occurring sections of message information ~~within said reduced data portion~~.

3. (Currently Amended) A method as in claim 1, wherein said analyzing ~~common content~~ comprises determining that increasing number of sources and destinations ~~that~~ are sending and/or receiving ~~within said portions~~ data.

4. (Currently Amended) A method as in claim 1, further comprising analyzing for the presence of a specified type of code within said collection of data.

5. (Currently Amended) A method as in claim 2, further comprising, after said analyzing determines said frequently occurring sections of message information, ~~then~~ carrying out an additional test on said frequently occurring sections of message information.

6. (Currently Amended) A method as in claim 5, wherein said carrying out the additional test is a test to comprises ~~look~~ looking for an increasing number of at least one of sources and destinations of said frequently occurring sections of message information.

7. (Currently Amended) A method as in claim 5, wherein said carrying out the additional test includes comprises a ~~test~~  
~~to look~~ looking for code within the frequently occurring sections.

8. (Currently Amended) A method as in claim 1, wherein said reducing said data ~~reduction~~ items includes comprises carrying out a hash function on said ~~portion of~~ data items.

9. (Currently Amended) A method as in claim 2, wherein said determining frequently occurring sections ~~is done by~~ comprises:

using at least first, second, and third data reduction techniques on each said ~~portion~~ data item[[,]] to obtain at least first, second and third ~~results~~ reduced data items;[[,]]

~~and to count~~ counting said first, second, and third ~~results~~ reduced data items;[[,]] and

~~to establish~~ establishing said frequently occurring sections when all of said at least first, second, and third ~~results~~ reduced data items have a frequency of occurrence greater than a specified amount.

10. (Currently Amended) A method as in claim 1, wherein said ~~portion~~ collection of data items ~~at least~~ includes comprises a portion of the network payload.

11. (Currently Amended) A method as in claim 5, wherein  
said carrying out the additional test comprises:  
maintaining a first list of unassigned addresses;  
forming a second list of sources that have sent to  
addresses on said first list; and  
comparing a current source of a frequently occurring  
section to said second list.

12. (Currently Amended) A method as in claim 11, wherein  
said ~~maintaining, and said forming, and said comparing, each~~  
carrying out the additional test comprise comprises data  
reducing information addresses in said first list and said  
second list to reduced addresses, wherein the reduced addresses  
have a smaller size and a constant predetermined relation with  
the addresses and at least some of the addresses that differ are  
reduced to the same reduced address.

13. (Currently Amended) A method as in claim 5, wherein  
said carrying out the additional test comprises:  
first monitoring a first content sent to a destination;  
second monitoring a second content sent by said  
destination; and  
determining a correlation between said first content and  
said second content ~~as said additional test.~~

14. (Currently Amended) A method as in claim 13, wherein:  
said first monitoring comprises monitoring multiple  
destinations[[],] ; and

    said second monitoring comprises monitoring multiple  
destinations during a different time period than said first  
monitoring.

15. (Currently Amended) A method as in claim 14, wherein  
said first and second monitoring comprises:

    data reducing information about said destinations[[],] ;  
and  
    storing at least one table about said data reduced  
information.

16. (Currently Amended) A method as in claim 10, wherein  
said portion collection of data items further includes comprises  
a portion of a network header.

17. (Currently Amended) A method as in claim 11, wherein  
said portion of a network header [[is]] comprises a port number  
indicating a service requested by a network packet.

18. (Currently Amended) A method as in claim 17, wherein  
said port number [[is]] comprises a source port or a destination  
port.

19. (Currently Amended) A method as in claim 1, wherein:  
said portion of data items comprises comprise a first  
subset of a network packet including payload and header; and  
the method further comprising comprises obtaining a second  
subset of the same network packet for subsequent analysis.

20. (Currently Amended) A method as in claim 1, further  
comprising forming a plurality of portions data items from each  
of a collection of network packet packets, each of said  
plurality of portions data items comprising a specified subset  
of the network packet packets.

21. (Currently Amended) A method as in claim 1, further  
comprising forming a plurality of portions data items from each  
of a collection of network packet packets, each of said  
plurality of portions data items comprising a continuous portion  
of payload[[,]] and information indicative of a port number  
indicating a service requested by [[a]] the network packet.[[.]]

22. (Currently Amended) A method as in claim 2, wherein  
said reducing said data items and said determining frequently  
occurring sections comprises:

    taking a first hash function of said portion data items;  
[[,]]

first maintaining a first counter, with a plurality of stages, and incrementing one of said stages based on an output of said first hash function;

taking a second hash function of said portion data items; and

second maintaining a second counter, with a plurality of stages, and incrementing one of said stages of said second counter based on an output of said second hash function.

23. (Currently Amended) A method as in claim 22, further comprising:

checking said one of said stages of said first counter and said one of said stages of said second counter against a threshold[[],]; and

identifying said portion a first reduced data item as associated with frequent frequently occurring content only when both said one of said stages of said first counter and said one of said stages of said second counter are both above said threshold.

24. (Currently Amended) A method as in claim 23, further comprising adding frequent content the first reduced data item to a specified frequent content buffer table.

25. (Currently Amended) A method as in claim 24, further comprising:

    taking at least a third hash function of said portion data items; [[,]] and

    incrementing a stage of at least [[the]] a third counter based on said third hash function,

    where said identifying identify said portion first reduced data item as associated with frequent frequently occurring content only when all of said stages of each of said first, second, and third counters are each above said threshold.

26. (Currently Amended) A method as in claim 22, further comprising:

    obtaining said portion data items by taking a first part of ~~the message~~ messages; [[,]] and

    subsequently obtaining [[a]] new portion data items by taking a second part of the ~~message~~ messages.

27. (Currently Amended) A method as in claim 26, wherein at least one of said hash functions [[is]] comprises an incremental hash function.

28. (Currently Amended) A method as in claim 3, wherein  
reducing said data reduction items comprises:

hashing at least one of the source or destination ~~address~~  
addresses [[,]] to form a collection of hash value values [[,]]  
;

first determining a unique number of said hash values[[,]]  
; and

second determining a number of said one of source or  
destination ~~numbers~~ addresses based on said first determining.

29. (Currently Amended) A method as in claim 28, wherein  
~~said counting further comprises comprising~~ scaling the hash  
value values prior to said second determining.

30. (Currently Amended) A method as in claim 29, wherein  
said scaling comprises:

scaling by a first value during a first counting  
session[[,]] ; and

scaling by a second value during a second ~~measurment~~  
measurement interval session.

31. (Currently Amended) A method as in claim 7, wherein  
said detecting code comprises:

looking for a first valid opcode at a first location[[,]] ;

based on said first valid opcode, determining a second location representing an offset [[of]] to said first valid opcode[[],] ; and

looking for a second valid opcode at said second location.

32. (Currently Amended) A method as in claim 31, further comprising establishing that the a first portion as section including includes code when a predetermined number of valid opcodes are found at proper distances.

33. (Currently Amended) A method as in claim 1, further comprising[[],] :  
determining a list of first computers that are susceptible to a specified attack[[],] ; and

monitoring only messages directed to said first computers for said specified attack.

34. (Currently Amended) The method of claim 33, where said monitoring comprises checking for a message that attempts to exploit a known vulnerability to which a computer is vulnerable[[],] as said specified attack.

35. (Original) A method as in claim 34, wherein said checking comprises checking for a field that is longer than a specified length.

Claims 36.-68. (Canceled)

69. (Currently Amended) A method for automatically identifying common content to use in identifying an intrusive network attack, comprising:

monitoring network content on a network[[],] and obtaining at least a portion portions of the data on said network;

data reducing said portion portions of the data using a data reduction function which reduces said portion portions of the data to [[a]] reduced data portion portions in repeatable manner[[],] such that each portion which has the same content is reduced to the same reduced data portion and at least some of the portions that differ are reduced to the same reduced data portion;

analyzing said reduced data portion portions to find network content which repeats a specified number of times[[],] and to establish said network content which repeats said specified number of times as frequent content;

identifying address information of said frequent content, wherein the address information which includes at least one of [[a]] source information or destination information for that characterizes the respective of sources and/or destinations[[],] of said frequent content[[],] and determining if a number of sources and/or destinations for of said frequent content is increasing; and

identifying the frequent content as associated with [[a]]  
the network attack[,]] based on said identifying and  
determining.

70. (Currently Amended) A method as in claim 69, wherein  
said monitoring network content comprises obtaining both [[a]]  
portion portions of the data on the network[,]] and [[a]]  
portnumber portnumbers indicating [[a]] service services  
requested by [[a]] network packet packets.

71. (Currently Amended) A method as in claim 70, wherein  
said obtaining a portion portions of the network data comprises:  
defining a window which samples a first portion of network  
data at a first time defined by in accordance with a position of  
the window[,]] ; and  
sliding said window to a second position at a second time  
which samples a second portion of said network data, wherein  
said second position [[that]] has a specified offset from the  
first portion.

72. (Currently Amended) A method as in claim 71, wherein  
said data reduction function [[is]] comprises a hash function.

73. (Currently Amended) A method as in claim 72, wherein  
said data reduction function [[is]] comprises an incremental  
hash function.

74. (Currently Amended) A method as in claim 69, wherein  
data reducing said portions comprises using said hash data  
reduction function is used in a scalable configuration.

75. (Currently Amended) A method as in claim 69, wherein  
said identifying comprises:

second data reducing said address information using a data  
reduction function[[],] ; and  
maintaining a table of data reduced address information.

76. (Original) A method as in claim 75, wherein said  
second data reducing comprises hashing said address information.

77. (Currently Amended) A method as in claim 69, further  
comprising testing contents of the ~~network packet associated~~  
~~with~~ the frequent content to determine the presence of code in  
said contents frequent content.

78. (Currently Amended) A method as in claim 77, wherein  
said testing contents comprises:

determining identifying an opcode in said contents frequent  
content [[],] ;  
determining a length of the opcode[[],] ; and  
looking for another opcode at a location within said  
contents frequent content based on said length.

79. (Currently Amended) A method as in claim 69, further comprising monitoring for scanning of addresses ~~associated with said frequent content~~.

Claims 80.-87. (Canceled)

88. (New) A method for automatically identifying common content to use in identifying an intrusive network attack, comprising:

obtaining a collection of data items to be analyzed to identify the network attack;

reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item;

analyzing a plurality of said reduced data items to determine frequently occurring sections of message information indicative of a network attack; and

carrying out an additional test on said frequently occurring sections of message information, comprising

maintaining a first list of unassigned addresses, wherein the unassigned addresses are maintained as reduced addresses that have a smaller size and a constant predetermined relation with the unassigned addresses and at least some of the unassigned addresses that differ are reduced to the same reduced address,

forming a second list of source addresses that have sent to the unassigned addresses on said first list, wherein the source addresses are maintained as reduced addresses that have a smaller size and a constant predetermined relation with the source addresses and at least some of the source addresses that differ are reduced to the same reduced address, and

comparing a current source of a frequently occurring section to said second list.

89. (New) A method for automatically identifying common content to use in identifying an intrusive network attack, comprising:

obtaining a collection of data items to be analyzed to identify the network attack, wherein said data items comprise a first subset of a network packet including payload and header;

reducing said data items in said collection to reduce said data collection to a reduced data collection of reduced data items, wherein the reduced data items in the reduced data collection have a smaller size and a constant predetermined relation with data items in the data collection and at least some of the data items in the data collection that differ are reduced to the same reduced data item;

analyzing a plurality of said reduced data items to detect common elements, said analyzing reviewing for common content indicative of a network attack; and

obtaining a second subset of the same network packet for subsequent analysis.